

PCT

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY



(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

REC'D 03 OCT 2005

WIPO

PCT

Applicant's or agent's file reference PD53581PC00	FOR FURTHER ACTION See Form PCT/PEA/416	
International application No. PCT/EP2004/009462	International filing date (day/month/year) 25.08.2004	Priority date (day/month/year) 02.09.2003
International Patent Classification (IPC) or national classification and IPC G06F1/00		
Applicant SONY ERICSSON MOBILE COMMUNICATIONS AB et al.		
<p>1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of 5 sheets, including this cover sheet.</p> <p>3. This report is also accompanied by ANNEXES, comprising:</p> <p>a. <input checked="" type="checkbox"/> sent to the applicant and to the International Bureau a total of 5 sheets, as follows:</p> <p><input checked="" type="checkbox"/> sheets of the description, claims and/or drawings which have been amended and are the basis of this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).</p> <p><input type="checkbox"/> sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.</p> <p>b. <input type="checkbox"/> (sent to the International Bureau only) a total of (Indicate type and number of electronic carrier(s)) , containing a sequence listing and/or tables related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).</p>		
<p>4. This report contains indications relating to the following items:</p> <p><input checked="" type="checkbox"/> Box No. I Basis of the opinion</p> <p><input type="checkbox"/> Box No. II Priority</p> <p><input type="checkbox"/> Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p><input type="checkbox"/> Box No. IV Lack of unity of invention</p> <p><input checked="" type="checkbox"/> Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p><input type="checkbox"/> Box No. VI Certain documents cited</p> <p><input type="checkbox"/> Box No. VII Certain defects in the international application</p> <p><input type="checkbox"/> Box No. VIII Certain observations on the international application</p>		
Date of submission of the demand 16.04.2005	Date of completion of this report 29.09.2005	
Name and mailing address of the international preliminary examining authority:  European Patent Office - Glitschiner Str. 103 D-10958 Berlin Tel. +49 30 25901 - 0 Fax: +49 30 25901 - 840	Authorized Officer Nazzaro, A Telephone No. +49 30 25901-403 	

**INTERNATIONAL PRELIMINARY REPORT
ON PATENTABILITY**

International application No.
PCT/EP2004/009462

Box No. I Basis of the report

1. With regard to the **language**, this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.
- ☐ This report is based on translations from the original language into the following language , which is the language of a translation furnished for the purposes of:
- ☐ international search (under Rules 12.3 and 23.1(b))
 - ☐ publication of the international application (under Rule 12.4)
 - ☐ international preliminary examination (under Rules 55.2 and/or 55.3)
2. With regard to the **elements*** of the international application, this report is based on *(replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report):*

Description, Pages

1-11 as originally filed

Claims, Numbers

1-27 received on 16.04.2005 with letter of 14.04.2005

Drawings, Sheets

1, 2 as originally filed

☐ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing

3. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages
- ☐ the claims, Nos.
- ☐ the drawings, sheets/figs
- ☐ the sequence listing (*specify*):
- ☐ any table(s) related to sequence listing (*specify*):

4. ☐ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

- ☐ the description, pages
- ☐ the claims, Nos.
- ☐ the drawings, sheets/figs
- ☐ the sequence listing (*specify*):
- ☐ any table(s) related to sequence listing (*specify*):

* If item 4 applies, some or all of these sheets may be marked "superseded."

**INTERNATIONAL PRELIMINARY REPORT
ON PATENTABILITY**

International application No.
PCT/EP2004/009462

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	1-27
	No: Claims	
Inventive step (IS)	Yes: Claims	1-27
	No: Claims	
Industrial applicability (IA)	Yes: Claims	1-27
	No: Claims	

2. Citations and explanations (Rule 70.7):

see separate sheet

Re Item V.

1 The following documents are referred to in this communication:

D1: US-A-6 115 819 (ANDERSON MARK STEPHEN) 5 September 2000 (2000-09-05)

2 INDEPENDENT CLAIM 1

Document D1, which is considered to represent the most relevant state of the art, discloses [the references in square brackets] applying to this document:

Method of transferring data from a non-volatile memory (24) to a working memory (22) of an electronic data processing device (10), comprising the steps of: copying security data (30) from the non-volatile memory to the working memory, which security data is to be write-protected, (steps 36; 50, 58), [see abstract and figure 1].

From this, the subject-matter of independent claim 1 differs in that:

The activation of a blocking function for the security data in the working memory is triggered by the copying being made to the working memory.

2.1 The subject-matter of claim 1 is therefore novel (Article 33(2) PCT)

The problem to be solved by the present invention may be regarded as:
how to protect security data which has been transferred from a non-volatile memory to a working memory.

2.2 The solution to this problem proposed in claim 1 of the present application is considered as involving an inventive step (Article 33(3) PCT) for the following reasons:

None of the available documents discloses the differing feature.

- 2.3 Claims 2-8 are dependent on claim 1 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

3 INDEPENDENT CLAIMS 9 AND 17

Independent claim 9 defines the device for blocking write attempts to security data corresponding to the method of claim 1 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

Independent claim 17 defines an electronic data processing device which includes a non-volatile memory, a working memory, a CPU and the device for blocking write attempts of claim 9 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

- 3.1 Claims 10-16 and 18-27 are dependent respectively on claims 9 and 17 and as such also meet the requirements of the PCT with respect to novelty and inventive step.

CLAIMS

1. Method of transferring data from a non-volatile memory (24) to a working memory (22) of an electronic data processing device (10), comprising the steps of:
- 5 copying security data (30) from the non-volatile memory to the working memory, which security data is to be write-protected, (steps 36; 50, 58), activating a blocking function for the security data in the working memory, (step 38; 52), which step of activating is triggered by the copying being made
- 10 to the working memory, monitoring all communication with the working memory, (steps 34, 42; 56), and blocking all write attempts to the copied security data stored in the working memory according to the blocking function, (steps 44; 60),
- 15 wherein at least the steps of activating a blocking function, monitoring communication and blocking write attempts are performed independently of the central processing unit (14) of the data processing device, such that the central processing unit cannot manipulate the security data.
- 20 2. Method according to claim 1, wherein the area (A1, A2) of the security data in the non-volatile memory is pre-defined and pre-stored in a device for blocking write attempts (16) and used at least in relation to activating a blocking function.
- 25 3. Method according to claim 1 or 2, wherein the step of copying data comprises copying only the security data from the non-volatile memory to the working memory independently of the central processing unit of the data processing device (step 50) and copying any further data under the control of the central processing unit of the device (step 58).
- 30 4. Method according to claim 3, wherein the area (A1, A2) of the security data in the non-volatile memory and the area (B1, B2) for storage of the security data in the working memory are pre-defined and wherein the step of activating a blocking function is triggered by the copying being made to the pre-defined area in the working memory and the blocking function is activated for that area
- 35 of the working memory.

5. Method according to claim 1 or 2, wherein the step of copying comprises copying all data from the non-volatile memory to the working memory under the control of the central processing unit of the device (step 36).

5 6. Method according to claim 5, wherein the area (A1, A2) of the security data in the non-volatile memory is pre-defined and wherein the step of activating a blocking function is triggered by a first detection of copying of security data from the pre-defined area in the non-volatile memory to an area (B1, B2) of the working memory and the blocking function is activated for that area of the
10 working memory.

7. Method according to any previous claim, wherein the blocking function comprises changing the destination address of the data transferred to the working memory.

15 8. Method according to any previous claim, further comprising the steps of disconnecting a debugging unit (step 32; 48) at least when copying the security data to the working memory and reconnecting the debugging unit (step 40; 54) when the blocking function has been activated.

20 9. Device (16) for blocking write attempts to security data (30) transferred from a non-volatile memory (24) to a working memory (22) in an electronic data processing environment (10) that includes a central processing unit (14) and comprising a monitoring unit (28) arranged to:
25 activate a blocking function for security data in the working memory, which activation is triggered by a copying of the security data being made from the non-volatile memory to the working memory,
monitor all communication with the working memory, and
block all write attempts to the copied security data stored in the working
30 memory according to the blocking function,
all performed independently of the central processing unit of the data processing environment such that the central processing unit cannot manipulate the security data.

35 10. Device according to claim 9, wherein the area (A1, A2) of the security data in the non-volatile memory is pre-defined and pre-stored in the device and used in relation at least to activating a blocking function.

11. Device according to claim 9 or 10, further comprising a copy control unit (46) arranged to copy the security data from the non-volatile memory to the working memory also independently of the central processing unit of the data processing environment.
12. Device according to claim 11, where the area (A1, A2) of the security data in the non-volatile memory and the area (B1, B2) for storage of the security data in the working memory are pre-defined and pre-stored in the device and the monitoring unit when activating a blocking function is triggered by the copying being made to the pre-defined area in the working memory and the blocking function is activated for that area of the working memory.
13. Device according to claim 9 or 10, where the area of the security data (A1, A2) in the non-volatile memory is pre-defined and pre-stored in the device and the monitoring unit when activating a blocking function is triggered by a first detection of copying of security data from the pre-defined area in the non-volatile memory to an area (B1, B2) of the working memory and the blocking function is activated for that area of the working memory.
14. Device according to any of claims 9 – 13, wherein the blocking function of the monitoring unit comprises blocking write attempts by changing the destination address of data transferred to the working memory.
15. Device according to any of claims 9 – 14, wherein the monitoring unit is arranged to disconnect a debugging unit (26) of the electronic data processing environment at least when the security data is copied to the working memory and to reconnect the debugging unit when the blocking has been activated.
16. Device according to any of claims 9 – 15, wherein it is implemented in hardware.
17. Electronic data processing device (10) comprising:
a non-volatile memory (24) comprising data including security data (30) to be write-protected,
a working memory (22),
a central processing unit (14) arranged to control copying of at least some data from the non-volatile memory to the working memory, and

a device for blocking write attempts (16) to security data transferred from the non-volatile memory to the working memory and comprising a monitoring unit (28) arranged to:

activate a blocking function for security data in the working memory, which activation is triggered by a copying of the security data being made from the non-volatile memory to the working memory,
monitor all communication with the working memory, and
block all write attempts to the copied security data stored in the working memory according to the blocking function,
all performed independently of the central processing unit, such that the central processing unit cannot manipulate the security data.

18. Electronic data processing device according to claim 17, wherein the area (A1, A2) of the security data in the non-volatile memory is pre-defined and pre-stored in the device for blocking write attempts and used in relation at least to activating a blocking function.

19. Electronic data processing device according to claim 17 or 18, wherein the device for blocking write attempts further comprises a copy control unit (46) arranged to copy the security data from the non-volatile memory to the working memory independently of the central processing unit and the central processing unit is arranged to control the copying of further data from the non-volatile memory to the working memory.

20. Electronic data processing device according to claim 19, where the area (A1, A2) of the security data in the non-volatile memory and the area (B1, B2) for storage of the security data in the working memory are pre-defined and pre-stored in the device for blocking write attempts and the monitoring unit when activating a blocking function is triggered by the copying being made to the pre-defined area in the working memory and the blocking function is activated for that area of the working memory.

21. Electronic data processing device according to claim 17 or 18, wherein the central processing unit is arranged to control the copying of all data from the non-volatile memory to the working memory.

22. Electronic data processing device according to claim 21, where the area (A1, A2) of the security data in the non-volatile memory is pre-defined and pre-

stored in the device for blocking write attempts and the monitoring unit when activating a blocking function is triggered by a first detection of copying of security data from the pre-defined area in the non-volatile memory to an area (B1, B2) of the working memory and the blocking function is activated for that area of the working memory.

23. Electronic data processing device according to any of claims 17 – 22, wherein the blocking function of the monitoring unit comprises blocking write attempts by changing the destination address of data transferred to the working memory.

24. Electronic data processing device according to any of claims 17 – 23, further comprising a debugging unit (26) and wherein the monitoring unit is arranged to disconnect the debugging unit at least when the security data is copied to the working memory and to reconnect the debugging unit when the blocking has been activated.

25. Electronic data processing device according to any of claims 17 – 24, wherein the device for blocking write attempts is implemented in hardware.

26. Electronic data processing device according to any of claims 17 – 25, wherein the device is a portable communication device.

27. Electronic data processing device according to claim 26, wherein the device is a cellular phone.

Box No. VIII (iv) DECLARATION: INVENTORSHIP (only for the purposes of the designation of the United States of America)
The declaration must conform to the following standardized wording provided for in Section 214; see Notes to Boxes Nos. VIII, VIII (i) to (iv) (in general) and the specific Notes to Box No. VIII (iv). If this Box is not used, this sheet should not be included in the request.

**Declaration of inventorship (Rules 4.17(iv) and 51bis.1(a)(iv))
 for the purposes of the designation of the United States of America:**

I hereby declare that I believe I am the original, first and sole (if only one inventor is listed below) or joint (if more than one inventor is listed below) inventor of the subject matter which is claimed and for which a patent is sought.

This declaration is directed to the international application of which it forms a part (if filing declaration with application).

This declaration is directed to international application No. PCT/..... (if furnishing declaration pursuant to Rule 26ter).

I hereby declare that my residence, mailing address, and citizenship are as stated next to my name.

I hereby state that I have reviewed and understand the contents of the above-identified international application, including the claims of said application. I have identified in the request of said application, in compliance with PCT Rule 4.10, any claim to foreign priority, and I have identified below, under the heading "Prior Applications," by application number, country or Member of the World Trade Organization, day, month and year of filing, any application for a patent or inventor's certificate filed in a country other than the United States of America, including any PCT international application designating at least one country other than the United States of America, having a filing date before that of the application on which foreign priority is claimed.

Prior Applications: EP 03019882.4
 US 60/501,630

I hereby acknowledge the duty to disclose information that is known by me to be material to patentability as defined by 37 C.F.R. § 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the PCT international filing date of the continuation-in-part application.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Name: LUTNAES, Sturla

Residence: Uppsala
 (city and either US state, if applicable, or country)

Mailing Address: Malma Ringv. 48
 SE-756 45 Uppsala, Sweden

Citizenship: NORWEGIAN

Inventor's Signature: Sturla Lutnaes
 (if not contained in the request, or if declaration is corrected or added under Rule 26ter after the filing of the international application. The signature must be that of the inventor, not that of the agent)

Date: 2004-07-07
 (of signature which is not contained in the request, or of the declaration that is corrected or added under Rule 26ter after the filing of the international application)

Name:

Residence:
 (city and either US state, if applicable, or country)

Mailing Address:

Citizenship:

Inventor's Signature:
 (if not contained in the request, or if declaration is corrected or added under Rule 26ter after the filing of the international application. The signature must be that of the inventor, not that of the agent)

Date:
 (of signature which is not contained in the request, or of the declaration that is corrected or added under Rule 26ter after the filing of the international application)

☐ This declaration is continued on the following sheet, "Continuation of Box No. VIII (iv)".